UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/679,268	10/07/2003	Anthony C. Fascenda	62922.4	3130

21967 7590 11/25/2008

HUNTON & WILLIAMS LLP
INTELLECTUAL PROPERTY DEPARTMENT
1900 K STREET, N.W.
SUITE 1200
WASHINGTON, DC 20006-1109

EXAMINER	
ARMOUCHE, HADI S	
ART UNIT	**PAPER NUMBER**
2432	

MAIL DATE	DELIVERY MODE
11/25/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/679,268	FASCENDA, ANTHONY C.	
	Examiner	Art Unit	
	HADI ARMOUCHE	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 September 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,5-8 and 12-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,5-8 and 12-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10/07/2003* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Specification

1. Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

2. The abstract of the disclosure is objected to because it exceeds 150 words (currently 181 words). Correction is required. See MPEP § 608.01(b).

3. The use of the trademark has been noted in this application. It should be capitalized wherever it appears and be accompanied by the generic terminology.

Although the use of trademarks is permissible in patent applications, the proprietary nature of the marks should be respected and every effort made to prevent their use in any manner which might adversely affect their validity as trademarks.

4. In paragraph 10 line 4, MICROSOFT WINDOWS is used. In paragraph 12 lines 5, 8 and 9, WAYPORT is used. In paragraph 13 lines 1, 2, 4, 6, 9, 10 and 13, BOINGO is used. In paragraph 41 line4, CRYPTOFLEX is used.

5. The disclosure is objected to because of the following informalities: in paragraph 1, applicant refers to the other related applications and indicates with 10/xxx,xxx for

their application number. Please insert 10/679,472 and 10/679,371. Moreover, applicant claims priority to a provisional application 60/447,921. It should be 60/477,921. Appropriate correction is required.

6. The lengthy specification has not been checked to the extent necessary to determine the presence of all possible minor errors. Applicant's cooperation is requested in correcting any errors of which applicant may become aware in the specification.

Drawings

7. Figure 5A is objected to as failing to comply with 37 CFR 1.84(p)(4) because reference character “550” has been used to designate both “Copy BBSID, MKS, and MKR to client Key" and "Exit". Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either “Replacement Sheet” or “New Sheet” pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Response to Arguments

8. Applicant's arguments with respect to claim 1 and similar claim 15 filed 09/30/2007 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 112

9. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

10. Claim 17 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The claim refers to IEEE 802.11 protocol. However, it is not clear which of the IEEE802.11 family protocols/standards it is.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 1-2 and 15-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Whelan et al (US. PGPub No. 2004/0198220), hereafter “Whelan” further in view of Menezes et al, “ Handbook of Applied Cryptography” book, 5th edition, June 2001, CRC press, Referred to hereinafter by Menezes.

12. With regard to claim 1 and similar claim 15, Whelan discloses method of authenticating a client to one ore more computing devices on one or more communications networks ([0063], lines 1-3), the method comprising the steps of:

obtaining, by the client, a computing device identifier (Fig. 1, item 28, [0032], lines 21-23, association list is downloaded that contains computing device identifier for each sub-net indicates obtaining an computing device identifier) associated with a computing device;

selecting, at said client (Fig. 1, item 28 mobile unit), a set of authentication parameters associated with said computing device identifier, with said computing device identifier, said authentication parameters ([0043], lines 5-8) being stored in a tamper-resistant physical token operatively coupled to said client, said tamper-resistant physical token further permanently storing a unique identifier associated with said client, said tamper resistant physical token further storing a first cryptographic key; and

implementing an authentication process employing said set of authentication parameters ([0049] lines 13-16, authenticate the access point reads on implementing an authentication process and the access point on the association list indicates authentication parameters).

permitting, at said client, said client to access said communications network via said computing device if said authentication process results in a successful authentication of said client (Fig. 2a and 2b, [0049] lines 8-16).

However, Whelan does not disclose explicitly that the authentication process comprising the steps of:

transmitting, by the client to the computing device, a first challenge, wherein said first challenge comprises an encrypted first random number and a unique identifier associated with said computing device, said encrypted first random number being encrypted with said first cryptographic key.

receiving, by the client from the computing device, a second challenge, wherein said second challenge comprises an encrypted second random number, said second random number generated at said computing device and encrypted with a second cryptographic key, said second cryptographic key being obtained by said computing device and associated with said computing device identifier.

Menezes teaches in protocol 12.39 on page 508 a modified Needham-Schroeder public key protocol wherein the client (A) sends B (the device) a challenge with r_1 and k_1 and the challenge is encrypted with P_B. Similarly for the challenge between the device and the client.

It would have been obvious to one of the ordinary skill in the art at the time of the Applicant's invention was made to modify the authentication process method of Whelan by a modified Needham-Schroeder public key protocol. The motivation/suggestion would have been to provide a mutual authentication between the client and the device communicating on a network.

13. With regard to claim 2, Whelan discloses said computing device identifier is a basic service set identifier (BSSID) ([0006], lines 1-5).

14. With regard to claim 16, Whelan discloses each client device further includes a wireless communications transceiver to communicate with one of said one or more computing devices via a wireless channel (Fig. 1, [0082] lines 1-6).

15. With regard to claim 17, Whelan discloses wireless channel (Fig. 1, item 26) is an IEEE 802.11 wireless channel ([0004] lines 1-4).

16. Claims 5-8, 12, and 18-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Whelan and Menezes in further in view of Balogh (US PGPub. No. 2001/0023446), hereafter “Balogh”.

17. With regard to claim 5, Whelan does not disclose installing the tamper-resistant physical token at the computing device. However, Balogh discloses installing the tamper-resistant physical token at the computing device ([0030], lines 7-9).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Whelan by installing the tamper-resistant physical token at the computing device, as taught by Balogh to allow users to connect to a network without knowing what settings are needed and how to change the settings ([0007] lines 1-3).

18. With regard to claims 6 and 22, Whelan does not disclose the tamper-resistant physical token is adapted to be inserted into a communications port at said client.

However, Balgoh discloses the tamper-resistant physical token is adapted to be inserted into a communications port at said client ([0030] lines 7-9, card reader indicates a communication port).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Whelan such that the tamper-resistant physical token is adapted to be inserted into a communications port at said client, as taught by Balogh to allow users to connect to a network without knowing what settings are needed and how to change the settings ([0007] lines 1-3).

19. With regard to claims 6 and 22, Whelan does not disclose the tamper-resistant physical token is adapted to be inserted into a communications port at said client. However, Balgoh discloses the tamper-resistant physical token is adapted to be inserted into a communications port at said client ([0030] lines 7-9, card reader indicates a communication port).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Whelan such that the tamper-resistant physical token is adapted to be inserted into a communications port at said client, as taught by Balogh to allow users to connect to a network without knowing what settings are needed and how to change the settings ([0007] lines 1-3).

20. With regard to claim 7, Whelan discloses one or more additional sets of authentication parameters ([0050] lines 4-5, temporary association list indicate one or more sets of authentication parameters), wherein each set of authentication parameters is associated with a unique access point identifier ([0051] lines 1-3).

However, Whelan does not disclose the tamper-resistant physical token further comprises one or more additional sets of authentication parameters, wherein each of the one or more additional sets of authentication parameters is associated with a unique computing device identifier.

Balogh, on the other hand, discloses the tamper-resistant physical token (Fig. 1, item SC, [0030] lines 4-7) further comprises one or more additional sets of authentication parameters, wherein each set of authentication parameters is associated with a unique computing device identifier.

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Whelan to include the tamper-resistant physical token, as taught by Balogh to allow users to connect to a network without knowing what settings are needed and how to change the settings ([0007] lines 1-3).

21. With regard to claim 8, Whelan discloses each of the unique computing device identifier is in relation to its associated set of authentication parameters (Fig. 1, item 34, [0042] 4-7).

However, Whelan does not discloses each of the unique computing device identifier is stored in said tamper-resistant physical token and in relation to its associated set of authentication parameters.

Balogh, on the other hand, discloses each of the unique computing device identifier is stored in said tamper-resistant physical token (Fig. 1, item SC, [0030] lines 4-7) and in relation to an associated set of authentication parameters.

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Whelan such that set of authentication parameters are pre-stored in a temper-resistant physical token, as taught by Balogh to allow users to connect to a network without knowing what settings are needed and how to change the settings ([0007] lines 1-3).

22. With regard to claim 12, Whelan disclose the unique identifier is a serial number ([0006], lines 3-4, BSSID uniquely identify an Access point indicates a serial number), but Whelan does not disclose a serial number of the tamper resistant physical token.

Balogh, on the other hand, discloses the tamper resistant physical token (Fig. 1, item SC, [0030] lines 4-7).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the authentication process method of Whelan by includes a serial number of the tamper resistant physical token, as taught by Balogh to allow users to connect to a network without knowing what settings are needed and how to change the settings (Balogh, [0007] lines 1-3).

23. With regard to claim 18, Whelan discloses one or more authentication devices (Fig. 1, item 10) but does not disclose one or more computing devices are Wi-Fi access points.

Balogh, on the other hand, disclose one or more authentication devices are Wi-Fi access points (Fig. 1, AP1-AP3).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the authentication process method of Whelan

by including one or more computing devices are Wi-Fi access points, as taught by Balogh to allow users to connect to a network without knowing what settings are needed and how to change the settings (Balogh, [0007] lines 1-3).

24. With regard to claim 19, Whelan discloses at least two Wi-Fi access points (Fig. 1, Item 28) but does not disclose at least two Wi-Fi access points are associated with different Wi-Fi networks are associated with different Wi-Fi networks.

Balogh, on the other hand, discloses at least two Wi-Fi access points are associated with different Wi-Fi networks (Fig. 1, Item AP1-4 with NW1 and NW2).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the communication system of Whelan by including at least two Wi-Fi access points are associated with different Wi-Fi networks, as taught by Balogh to allow users to connect to a network without knowing what settings are needed and how to change the settings (Balogh, [0007] lines 1-3).

25. With regard to claim 20, Whelan discloses each of the one or more unique sets of authentication parameters is associated with an access point identifier ([0043], lines 5-8).

26. With regard to claim 21, Whelan discloses said computing device identifier is a basic service set identifier (BSSID) ([0006], lines 1-5).

27. Claims 13-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Whelan and Menezes in further in view of Nevoux et al. (US Pat. No. 5661806), hereafter “Nevoux”.

28. With regard to claim 13, Whelan discloses the set of authentication parameters ([0043], lines 5-8), further comprises: a network (Fig. 1, item 18, [0042] lines 1-3)

However, neither Whelan nor Balogh discloses a network receive cryptographic key and a network send cryptographic key.

Nevoux, on the other hand, discloses a network receive cryptographic key (Fig. 2 VLR column, receiving SRES indicates receive cryptographic key) and a network send cryptographic key (Fig. 2, HLR Column, sending Ks which is a result of the AG encryption function, reads on send cryptographic key).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the methods of Whelan and Balogh by including a network receive cryptographic key and a network send cryptographic key in the set of authentication parameters, as taught by Nevoux to avoid unauthorized access from mobile stations of malicious intruders in a radio-based wireless LAN system.

29. With respect to claim 14, Whelan further discloses the first challenge (Fig. 2A, item 50, initiates association indicates first challenge) and the second challenge (Fig. 2A, item 66, since the outcome of the decision branch of Item 66 feed the response back to the MU indicating there are more AP available; it reads on second challenge), and decrypting the second challenge ([0075] lines 1-7).

However, neither Whelan nor Balogh discloses encrypting, by the client, the first challenge with the network send cryptographic key; and decrypting the second challenge with the network receive cryptographic key.

Nevoux, on the hand, discloses encrypting said first challenge with said network send cryptographic key (Fig. 2, HLR column item Ks, sending Ks which is an encrypted cryptographic key from a network indicates network send cryptographic key) and network receive cryptographic key (Fig. 2 VLR column, receiving SRES indicates receive cryptographic key)

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the methods of Whelan and Balogh to include in the authentication parameters further comprises the step of encrypting said first challenge with said network send cryptographic key, as taught by Nevoux to avoid unauthorized access from mobile stations of malicious intruders in a radio-based wireless LAN system.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to HADI ARMOUCHE whose telephone number is (571)270-3618. The examiner can normally be reached on M-Th 7:30-5:00 and Fridays half day.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/H. A./
HADI ARMOUCHE
Examiner, Art Unit 2432

/Benjamin E Lanier/
Primary Examiner, Art Unit 2432